UNITED STATES MARINE CORPS
C Company
Marine Corps Communication-Electronics School
Marine Corps Air Ground Combat Center
Box 788251
Twentynine Palms, California 92278-5020

Student Handout
(SH)

Marine Air Command and Control System 200 Level
Training and Readiness (T&R) Instruction

LESSON DESIGNATOR: A-18

LESSON TITLE: ENCRYPTION/AUTHENTICATION PROCEDURES

I. ENABLING LEARNING OBJECTIVES:

A. Without the aid of, but in accordance with the references, select the number of characters that can be encrypted without changing the set indicator.

B. Without the aid of, but in accordance with the references, select the maximum period of time that used pages of an AKAC 874B may be retained before they must be destroyed.

C. Given an AKAC 874B and a KAL 61C, without the aid of, but in accordance with the references, reply to an authentication challenge.

D. Given an AKAC 874B and a KAL 61C, without the aid of, but in accordance with the references, determine the set letter, once given the set indicators.

E. Given an AKAC 874B and a KAL 61C, without the aid of, but in accordance with the references, encrypt grid coordinates including grid zone designators.

F. Given an AKAC 874B and a KAL 61C, without the aid of, but in accordance with the references, demonstrate how to authenticate.

G. Given an AKAC 874B and a KAL 61C, without the aid of, but in accordance with the references, use gingerbread procedures.

II. LESSON PLAN /OVERVIEW: The purpose of this period of instruction is to teach you the proper way to correctly identify friendly units, and not be deceived by the enemy.

III. STUDENT INSTRUCTIONS:

A. Read the handout.

B. Attend the lecture.

C. Complete the homework.

IV. PRESENTATION OUTLINE:

A. Authentication.

1. The method of correctly identifying a station on the radio by a challenge and reply system. The steps to correctly authenticate are:

a. The station being called will look on the AKAC 874B and randomly select a two letter challenge, reading from left to right.

b. The station that initiated the original call will give a single letter response, found on the AKAC 874B on the line below the challenge and directly under the second letter of the challenge.

c. Once this is completed, the station who initiated the call will then issue a challenge to the station called and complete the procedure.

2. If the first letter of the challenge is found on the "Y" line, which is the last line on the AKAC 874B, then the response is found on the "A" line, which is the first line of the AKAC 874B.

B. Gingerbread Procedures.

1. The purpose of authentication on a radio net is to ensure that the enemy is not intruding on the net and trying to deceive us. Even if we are vigilant in our communication security procedures, the enemy will likely be no less vigilant in his attempts to deceive us. Therefore, we have an operational mechanism in place to immediately alert everyone on the net whenever an intrusion is detected. This mechanism is called gingerbread procedures.

2. . "Gingerbread" is actually a proword, as you should remember from your R/T class. Whenever you hear the proword "Gingerbread" on a radio net you know that some other operator on the net has identified a bogey station on the net.

3. There are two other items of information you need to listen for after you hear a gingerbread called:

a. The call sign of the bogey station.

b. A correct time authentication.

4. A typical example would sound like this:

a. C2E this is E9L, over.

b. E9L this is C2E, authenticate _ _, over

c. If E9L is unable or unwilling to correctly respond to the challenge three consecutive times, then the following gingerbread call is made: "All stations this net, this is C2E, GINGERBREAD GINGERBREAD E9L. I time authenticate _ _, C2E out."

C. Decryption

1. Decryption is the process of clarifying information that has been encrypted so the unit has usable data. This process is just the opposite of encryption.

2. The steps for decryption are:

a. After receiving the "Set Indicator" and the encrypted message, find the "Set Letter" and place the reader guide over the "Set Letter" as explained earlier.

b. The letters that are ciphered are found on the AKAC 874B inside the reader guide.

c. Write down the plain text numbers or letters that are found directly above or below the ciphered letters.

D. Encryption

1. The method of passing numbers and certain letters in a secure mode utilizing the AKAC 874B and the KAL 61C is called encryption. It is important to remember that we should never encrypt enemy coordinates or any information that is known to the enemy, for fear of compromise of the system. Always encrypt friendly locations and movements. The steps for encryption are:

a. Randomly select 2 letters as a "Set Indicator", from the AKAC 874B.

b. Once the "Set Indicator" has been selected, look directly to the right of the second letter of the "Set Indicator" to find the "Set Letter".

c. Place the reader guide so that the "Set Letter" is found between the arrow and the word SET on the reader guide.

d. The numbers or letters you wish to encrypt are found on the reader guide in plain text. The letters found inside the reader guide directly below or above the numbers or letter you wish to encrypt are the letters that you would write down as encryption. If you encrypt the same numeral more than once during a single transmission, select a different letter for encryption each time. The only letters that will be encrypted are grid zone designators.

2. As an operator, you will never use more than 15 characters be encrypted without changing the set indicator.

E. Time Authentication

1. Transmission authentication is used to validate the authenticity of a message only when it is impossible or impractical to use the challenge and reply authentication. Each authenticator is a two-letter response. The steps for time authentication are:

a. Note the actual time of transmission.

b. Locate the column on the effective table which is headed by the 2 digit number corresponding to the current hour.

c. Proceed down the column to the 2 digit number corresponding to the current number of minutes past the hour and give the 2 letter response.

d. If the current number of minutes past the hour is an odd number, subtract 1 minute. For example, if the time is 27 minutes after the hour, then use the 2 letter response for 26 minutes. The only allowable leeway is 4 minutes late at time of receipt.

F. Security

1. The Pacific Numeral Cipher/Authentication System is used worldwide so the security of this system is paramount. The individual who signs for the actual pages is responsible to ensure that it is secure and that each page of the publication is present. If any pages are missing, it should immediately be brought to the attention of the CMS custodian.

2. The operating instructions and handling instructions become at least "CONFIDENTIAL" when the effective date or the supersession date is filled in on the front cover. Remember, if you compromise this system, it is compromised throughout the world. Security of this system is a must!

3. <u>General Usage Rules</u>

a. Never encrypt more than 15 characters without changing the "Set Indicator".

b. Never encrypt information and then pass it in the clear.

c. Change the sheets of the AKAC 874 at the proper time.

d. Take the next month's AKAC 874B sheets when you deploy (in addition to the present month).

e. Do not write on the page.

f. Maintain control of the system.

4. <u>Destruction</u>

a. The individual pages will be destroyed as soon as possible after they expire, but no later than 72 hours. An entry into the SAD logbook is a minimum means of recording the destruction. Each unit in the Marine Air Command and Control System will have their own procedures to account for the destruction. Wherever recorded, double signatures (meaning two different people) are required.

b. A new system is being used out in the Fleet at this time is called the "TRIAD SYSTEM". This is how it works, you will be given (3) three letters vice (2) two. Instead of asking to "Authenticate Alpha Bravo," you will ask to "Authenticate Alpha Bravo Charlie."

V. <u>DEMONSTRATION/APPLICATION</u>: N/A.

VI. <u>SUMMARY/DEBRIEF</u>: During this period of instruction, we learned how to identify a friendly unit and communicate

VII. <u>REFERENCES</u>:

AKAC 874B Handling and Operating Instructions
CSP 1-A

Date last updated: 12 Dec 97